UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES	*	
	*	
v.	*	Criminal Action No. 1:20-cr-10012-IT
	*	
PAUL BATEMAN,	*	
	*	
Defendant.	*	

ORDER

November 16, 2022

TALWANI, D.J.

Defendant Paul Bateman seeks reconsideration of the court's decisions, Mem. & Order [Doc. No. 85]; Mem. & Order [Doc. No. 117], denying his Motion to Compel Discovery [Doc. No. 76] (sealed) and Motion to Suppress Evidence [Doc. No. 106]. Defendant contends that new information supports the earlier motions. After review of the additional material, the court finds no basis for further relief.

I. Background

The background of this dispute is set forth in the court's earlier decisions and need not be repeated in detail here. See Mem. & Order 2-3 [Doc. No. 85]; Mem. & Order 1-2 [Doc. No. 117]. At issue is a tip from a foreign law enforcement agency ("FLA" or "foreign agency") regarding a U.S. IP address connected to Bateman that had been used to access a child pornography website and the related information Homeland Security Investigations ("HSI") Special Agent Squire presented in an affidavit in support of an application for a warrant to search Bateman's home for evidence of child pornography. Squire Aff. ¶¶ 2, 4 [Doc. No. 76-4] (sealed).

After the government provided Bateman with its automatic discovery production, including, among other things, the search warrant and Squire's supporting affidavit, see Status

Report [Doc. No. 21], Bateman filed a his motion to compel seeking disclosure of the identity of members of the multinational group working to combat child exploitation referenced in Agent Squire's affidavit, information regarding the FLA's investigative technique used to identify the U.S. IP address, information as to the location of the Consulate General from which the FLA's tip was sent, and documentation of communication between the FBI and HSI regarding the FLA tip. The court denied the motion, finding Bateman's argument "based entirely on speculation that the evidence may show wrongdoing by foreign and domestic law enforcement." See Mem. & Order 7 [Doc. No. 85].

The government subsequently provided Bateman some additional information but continued to decline to identify the FLA that seized the server that hosted Website A[1] or the server host's country. See Mot. to Suppress 5 [Doc. No. 106]. Thereafter, Bateman filed his motion to suppress in which he argued that: the tip from the FLA was insufficient and the warrant was stale; Agent Squire made material omissions and misstatements in his affidavit about the tip, the methods used by the foreign agency to identify the IP address, and the relationship between the foreign agency and U.S. law enforcement; and he was for these reasons entitled to a Franks hearing. The court rejected each argument and denied the motion. See Mem. & Order [Doc. No. 117].

[1] The court has previously described Website A as "a child pornography site that operated on Tor as a hidden service—a website accessible only to users operating within the Tor network—from at least September 2016 through June 2019." Mem. & Order 1 [Doc. No. 85]. "Tor" refers to "the onion router," a network that facilitates efforts to anonymize communications over the Internet by routing user communications through a globally distributed network of intermediary computers. Squire Aff. ¶ 6 [Doc. No. 76-4] (sealed).

II. Standard

"A district court may grant a motion for reconsideration 'if the moving party presents newly discovered evidence, if there has been an intervening change in the law, or if the movant can demonstrate that the original decision was based on a manifest error of law or was clearly unjust.'" United States v. Cintron, 724 F.3d 32, 36 n.5 (1st Cir. 2013) (quoting United States v. Allen, 573 F.3d 42, 53 (1st Cir. 2009)). "The granting of a motion for reconsideration is 'an extraordinary remedy which should be used sparingly.'" Palmer v. Champion Mortg., 465 F.3d 24, 30 (1st Cir. 2006) (quoting 11 C. Wright, A. Miller & M. Kane, Federal Practice and Procedure § 2810.1 (2d ed. 1995)). "Unless the court has misapprehended some material fact or point of law, such a motion is normally not a promising vehicle for revisiting a party's case and rearguing theories previously advanced and rejected." Id.

III. Discussion

Bateman contends that recently discovered information supports his contention that the search warrant lacked probable cause and that Agent Squire made material omissions in his affidavit regarding his connection to foreign agencies.

A. *Multiple Cases Relied on an August 2019 Tip*

Bateman identified multiple cases from across the country that rely on an August 2019 tip from an unnamed FLA stating that an IP address was used to view a Tor hidden website in either April or May 2019. See Mot. for Reconsideration 2 [Doc. No. 126]. Bateman argues that these cases and related documents demonstrate that the FLA tip regarding the IP address referenced in Agent Squire's affidavit was part of a much wider, undisclosed investigation, and that the scale of the investigation calls into question the undisclosed methodology used to "de-anonymize the IP address." Id. Bateman's reasoning is not compelling. That the FLA was investigating the Tor network more generally and had provided more than one tip to U.S. law enforcement does not

undermine Agent Squire's affidavit in any way. Indeed, the affidavit disclosed that "[t]here is a long history of . . . FLA sharing criminal investigation information with U.S. law enforcement, . . . including the investigation of crimes against children," Squire Aff. 13, n.6 [Doc. No. 76-4] (sealed), and that "tips provided by FLA regarding IP addresses that FLA advised were associated with access to Tor network child exploitation-related web and chat sites" had led to the identification and arrests of other U.S. based individuals associated with child pornography production, trafficking and possession, id. at ¶ 26 (emphasis added). Nor does it logically follow that the multiple tips provided in August 2019 somehow undermine the methodology used to tie the specific IP address in question to Bateman.

B. *U.S. Law Enforcement was Working Closely and Collaboratively with Foreign Law Enforcement Agencies*

Bateman also argues that information he has obtained demonstrates that Agent Squire misstated the scale of the investigation of Website A and U.S. law enforcement's role in it.

Bateman presents: (1) FBI investigative documents dated January 2017, to show that the FBI was involved in a preliminary investigation into "Tor Hidden Service"; (2) documents from a foreign criminal case to tie the Department of Homeland Security, Agent Squire and HSI Boston to a joint international investigation of Tor hidden service sites as early as 2016; and (3) a similar complaint filed in the Western District of Washington[2] that claims that there was a "collaborative" investigation with foreign law enforcement that produced information regarding individuals accessing "dark web" sites through the Tor, and that alleges that the administrative

[2] United States v. Clark, 21-mj-00147-JLW (W.D. Wash. Mar. 11, 2021).

subpoenas were sent to internet service providers at similar times as in this case.[3] Mot. for Reconsideration 3, 5, 6 [Doc. No. 126]. However, these documents are not sufficient evidence that the "collaborative" investigation was the same in both cases.

Fourth, Bateman contends that the Clark complaint [Doc. No. 126-4] reveals that Agent Squire omitted that he was involved in the investigation of the Tor hidden sites prior to the June 2019 FLA seizure of Website A. Id. at 6. The Clark complaint states that "HSI Special Agent Greg Squire…observed the TARGET WEBSITE[4] while it was operational." Mot. for Reconsideration Ex. 4 ¶ 8 [Doc. No. 126-4]. In his affidavit in this case, Agent Squire stated that he received a tip from an FLA that "on April 30, 2019… IP address 73.142.30.140 was used to access online child sexual abuse and exploitation material via a website." See Squire Aff. ¶ 23 [Doc. No. 76-4] (sealed). The affidavit noted that the FLA was "known to U.S. law enforcement and [had] a history of providing reliable, accurate information in the past." Id. The fact that Agent Squire was able to view a target website prior to its seizure in June 2019 does not lend any support to the contention that the affidavit was false or materially misleading. That is, just because Agent Squire may have been able to observe an unnamed website on the same network does not indicate that he was able to access user data on that website. Further, not only does the Clark complaint not mention whether the two websites were in fact the same, but also the affidavit does not shy away from the fact that "[t]here is a long history of U.S. law enforcement

---

[3] Law enforcement sent an administrative subpoena on September 5, 2019, in the Clark case, see Mot. for Reconsideration Ex. 4 ¶ 10 [Doc. No. 126-4], and on September 10, 2019, in the instant case, see Squire Aff. ¶ 27 [Doc. No. 76-4] (sealed).

[4] There is no evidence to suggest that the "TARGET WEBSITE" from the Clark complaint is Website A from the instant case; however, both were accessed on the Tor network. See Mot. for Reconsideration 6 [Doc. No. 126] (redacted), [Doc. No. 126-14] (sealed).

sharing criminal investigation information with FLA and FLA sharing criminal investigation information with U.S. law enforcement." Id. at n.6.

Fifth, Bateman contends a case from outside the district which indicates that HSI Boston was working with foreign law enforcement agencies to investigate Tor networks as early as 2018 supports a finding that Agent Squire's affidavit contained misstatements as to the relationship between the United States and foreign agencies. See Mot. for Reconsideration 7-8 [Doc. No 126]. In that case from the Eastern District of Virginia, an affidavit in support of the complaint stated that "HSI Boston is also conducting an investigation of various Darkweb sites along with foreign law enforcement partners" in which "HSI Boston Agents requested information from foreign law enforcement partners for more information regarding the individual using [unnamed screennames]." Mot. for Reconsideration Ex. 8 ¶¶ 13, 16 [Doc. No. 126-8]. Once again, the presence of ongoing or concurrent investigations has no bearing on whether the affidavit in this case was false. Probable cause as required in an affidavit "is not a high bar," Kaley v. United States, 571 U.S. 320, 338 (2014), and "[i]t does not require the fine resolution of conflicting evidence that a reasonable-doubt or even a preponderance standard demands," Gerstein v. Pugh, 420 U.S. 103, 121 (1975). As such, Agent Squire was under no obligation to disclose the history of the agency's work beyond the scope of this case.

Sixth, Bateman contends that the United States v. Stauffer, Case No. 20-MJ-4005, RJD (S.D. Ill. Jan. 28, 2020), criminal complaint [Doc. No. 126-15] (sealed) reveals that U.S. law enforcement was in possession of a searchable copy of Website A as early as January 2020. See Mot. for Reconsideration 7 [Doc. No. 126-14] (sealed). In Stauffer, the government claimed that on January 10, 2020, the FBI Child Exploitation Operations Unit was able to provide the online

activity of Stauffer's username on Website A[5] from November 2016 to July 2018. Mot. for Reconsideration Ex. 7 ¶ 13 [Doc. No. 126-15] (sealed). Neither the Stauffer complaint nor Bateman's Motion [Doc. No. 126] provide any information as to *how* the FBI was able to search Website A in that case. Bateman alleges that the FBI must have received a searchable copy of the website from an FLA. However, that allegation remains speculative. The Stauffer complaint does not describe how the FBI was able to obtain Stauffer's online activity on the dark web, and without such information, Bateman's contention falls short.

Through the introduction of these documents, Bateman asks the court to infer that because U.S. law enforcement was aware of child pornography websites on the Tor network as early as 2016, there was a joint venture between the United States and other foreign agencies. That U.S. law enforcement was able to search Website A in January 2020, after the tip and affidavit in this case, does not have any relevance here.

In sum, the evidence provided does not sufficiently support Bateman's proposed inferences as to reconsider this court's decision. See Azubuko v. MBNA Am. Bank, 2005 WL 8176185, at *2 (D. Mass. Nov. 22, 2005) ("A motion for reconsideration should not 'give the losing party the opportunity to simply reargue its losing points and authorities.'") (quoting Coffin et al. v. Bowater Inc. et al., 2005 WL 3021979 at *1 (D. Me. Nov. 10, 2005)).

C. *The Use of Network Investigative Techniques to Identify Users on the Tor Network*

Bateman also contends that the alleged scale of the operation "calls into question not just the methodology used to de-anonymize the IP addresses, but the reliability of that as-yet

[5] The website at issue in Stauffer was identified as "Website A" in the Agent Squire Affidavit. See Mot. for Reconsideration 3 [Doc. No. 126-14] (sealed).

undisclosed methodology." See Mot. for Reconsideration 2 [Doc. No. 126]. Bateman also asks the court to reconsider its holding with respect to the alleged use of a Network Investigative Technique ("NIT") to access Bateman's IP address. As previously discussed, see Mem. & Order [Doc. No. 85], a NIT essentially amounts to a government installation of malware on a user's computer. See, e.g., United States v. Tagg, 886 F.3d 579, 583 n.2 (6th Cir. 2018). However, the use of such techniques qualifies as a Fourth Amendment search and requires a search warrant. See id. at 584; see also United States v. Anzalone, 208 F. Supp. 3d 358, 366 (D. Mass. 2016), aff'd, 923 F.3d 1 (1st Cir. 2019) ("Even if the defendant did not have a reasonable expectation of privacy in [his IP address], he did have a reasonable expectation of privacy in the computer that housed this data and that was instructed by the NIT to transmit the data back to the government.").

Bateman contends that because cases from across the country contain affidavits [Doc. Nos. 126-1 through 126-6] with similar facts, i.e., tips from an FLA regarding an IP address accessing child exploitation materials, there was a single, large operation. See, e.g., Mot. for Reconsideration Ex. 2 [Doc. No. 126-2] (alleging that in August 2019, the FBI received information from an FLA regarding an IP address that accessed a Tor hidden network on May 24, 2019); id. at Ex. 3 [Doc. No. 126-3] (alleging that in August 2019, the FBI received information from an FLA regarding an IP address that accessed a Tor hidden network on April 12, 2019); id. at Ex. 7 [Doc. No. 126-15] (sealed) (alleging that in August 2019, the FBI received information from an FLA regarding an IP address that accessed a Tor hidden network on April 29, 2019). Bateman then goes on to argue that because the operation was so large, a NIT was necessarily used. However, Bateman simply rehashes the same argument from his Motion to

Compel Discovery [Doc. No. 76] (sealed) that this court reviewed and rejected. See Mem & Order [Doc. No. 85].

D. *The Searchability of Links on the Tor Network*

Bateman contends that alternative descriptions of indexing on the Tor network entitles him to a Franks hearing on the ground that the affidavit lacked probable cause regarding his alleged criminal activity. See Mot. for Reconsideration 10-11 [Doc. No. 126]. Specifically, he references an affidavit from an investigator with the Federal Public Defender's Office from the Western District of New York [Doc. No. 126-13] that describes how a user can find links of hidden Tor websites through a search engine such as Google. Bateman contends that this information warrants reconsideration based on the idea that an individual could have accessed the homepage of Website A without being aware of its content, and that Agent Squire's characterization of the searchability of the Tor network entitles Bateman to a Franks Hearing.

However, Agent Squire's Affidavit [Doc. No. 76-4] (sealed) never claimed that it was impossible to access Website A through a search engine. Rather, the affidavit merely states that "[h]idden service websites on the Tor Network are not 'indexed' by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest." Squire Aff. ¶ 13 [Doc. No. 76-4] (sealed) (emphasis added). In addition, the affidavit notes that Website A was listed on "directory sites advertising hidden services dedicated to the sexual exploitation of children." Id. The possibility of accessing Website A through various methods, which both affidavits acknowledged, does not change the court's previous assessment that there was no material omission in the affidavit or error with the Magistrate Judge's probable cause determination. See Mem. & Order 7 [Doc. No. 117]; see also Illinois v. Gates, 462 U.S. 213, 236

(1983) ("[S]o long as the magistrate had a 'substantial basis for... conclud[ing]' that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more.") (quoting Jones v. United States, 362 U.S. 257, 271 (1960)).

IV. Conclusion

For the forgoing reasons, Bateman's Motion for Reconsideration [Doc. No. 126] is DENIED.

IT IS SO ORDERED.

November 16, 2022

/s/ Indira Talwani
United States District Judge